

AO 442 (12/85) Warrant for Arrest

2057126

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

UNITED STATES OF AMERICA,

WARRANT FOR ARREST

v.

ROMAN SELEZNEV
(Agent to Arrest)

CASE NO. 1:09-CR-491-SCJ-LTW

To: The United States Marshal
and any Authorized United States Officer

YOU ARE HEREBY COMMANDED to arrest ROMAN SELEZNEV and bring him or her
forthwith to the nearest magistrate to answer a(n)

☒ Indictment ☐ Information ☐ Complaint ☐ Order of Court ☐ Violation Notice ☐ Probation Violation Petition

Charging him or her with (brief description of offense): Wire Fraud
in violation of Title 18, United States Code, Section(s) 1343 and 2.

JAMES N. HATTEN
Name of Issuing Officer

Clerk, U.S. District Court
Title of Issuing Officer

B. HATTEN
Signature of Issuing Officer

December 22, 2014 at Atlanta, Georgia
Date and Location

Bail Fixed at \$ _____

By: _____
Name of Judicial Officer

RETURN

This warrant was received and executed with the arrest of the above-named defendant at:

Date Received: _____

Name and Title of Arresting Officer

Date of Arrest: _____

Signature of Arresting Officer

04385-093

DEC 22 14 PM 4:46 USMS NGA

ORIGINAL

FILED IN CHAMBERS
U.S.D.C. Atlanta

DEC 22 2014

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

JAMES H. HATTEN, Clerk
By: *B. J. Hatten* Deputy Clerk

ATLANTA DIVISION

UNITED STATES OF AMERICA	:	
	:	
v.	:	CRIMINAL INDICTMENT
	:	(Fourth Superseding)
	:	
VIKTOR PLESHCHUK,	:	
OLEG COVELIN,	:	NO. 1:09-CR-491-SCJ-LTW
IGOR GRUDIJEV,	:	
RONALD TSOI,	:	
EVELIN TSOI,	:	
MIKHAIL JEVGENOV,	:	
EVGENIY ANIKIN,	:	
previously charged as HACKER 3,	:	
VLADIMIR VALERYEVICH TAILAR	:	
aka Vladimir Taliar,	:	
aka Vladimir Taylar,	:	
aka Vladimir Talyar, and	:	
ROMAN SELEZNEV	:	

THE GRAND JURY CHARGES THAT:

COUNT ONE
(Conspiracy to Commit Wire Fraud)

1. From at least on or about November 4, 2008, through at least on or about November 25, 2008, in the Northern District of Georgia and elsewhere, the Defendants, VIKTOR PLESHCHUK, OLEG COVELIN, EVGENIY ANIKIN, together with others known and unknown to the Grand Jury, including, but not limited to, Sergei Tšurikov, Vladislav Horohorin, Ezenwa Chukukere, and Sonya Martin, did knowingly conspire to devise a scheme and artifice to defraud, and to obtain money and property, by means of material false and fraudulent pretenses, representations, and promises, and for the purpose of

executing such scheme and artifice, and attempting to do so, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain signs, signals, and sounds, that is, to knowingly cause computer commands to be transmitted from outside of the United States to the computer network of RBS WorldPay in the Northern District of Georgia, and to knowingly conduct and cause to be conducted ATM withdrawals using fraudulently obtained prepaid payroll card numbers and PIN codes from ATM terminals outside of the State of Georgia that were processed on computers within the Northern District of Georgia, in violation of 18 U.S.C. § 1349.

BACKGROUND

2. At all times relevant to this Indictment, unless otherwise indicated:

(a) RBS WorldPay (RBSW) was headquartered in Atlanta, in the Northern District of Georgia. RBS WorldPay was a wholly owned subsidiary of Citizens Financial Group (CFG), a bank holding company as defined in the Federal Deposit Insurance Act.

(b) RBS WorldPay processed credit and debit card transactions on behalf of financial institutions. The transactions occurred throughout the world and were processed by electronic means. RBS WorldPay's computer servers were located in the Northern District of Georgia.

(c) One of the services offered by RBS WorldPay was the processing of prepaid payroll card transactions. Prepaid payroll cards were debit cards funded through direct deposits from card holders' employers. Prepaid payroll cards allowed employers to pay their employees through direct deposits to prepaid payroll card accounts, instead of using paychecks or direct deposits into employees' bank accounts. Cash could be withdrawn by presenting the prepaid payroll card to an automated teller machine and entering the card's PIN code. Prepaid payroll cards could also be used to purchase goods and services from participating merchants. Transactions associated with these cards were processed by RBS WorldPay on behalf of its client financial institutions. Information related to these transactions was maintained by RBS WorldPay on the company's computer network.

(d) RBS WorldPay processed the transactions associated with prepaid debit cards issued by the following banks: RBS Citizens, N.A.; Palm Desert National Bank; The Bankcorp, Inc.; and First Bank of Delaware. Each of these issuing banks is federally insured. In addition to being a federally insured financial institution, RBS Citizens, N.A., is a member bank of the Federal Reserve System.

CONSPIRATORS

3. (a) Defendant PLESHCHUK was a computer hacker who during the relevant time period resided in or around St. Petersburg, Russia.

Based on Tšurikov's reconnaissance, Defendant PLESHCHUK manipulated the data on the RBS WorldPay computer network, with support from Defendants COVELIN, ANIKIN, and others, including, but not limited to, Tšurikov. Defendant PLESHCHUK with the support of Tšurikov developed the method by which the conspirators reverse engineered Personal Identification Numbers (PINs) from the encrypted data on the RBS WorldPay computer network. Defendant PLESHCHUK, with assistance from Tšurikov, Defendant ANIKIN, and others, raised the limits on certain of the prepaid payroll cards. Defendant PLESHCHUK and Tšurikov accessed the RBS WorldPay computer network and observed the withdrawals taking place on the cards they fraudulently obtained and distributed, tracking the proceeds of the fraud. Overall, Defendant PLESHCHUK managed the activities on the RBS WorldPay computer database, including modification of withdrawal limits, locking the cards so that there could be no further withdrawals, and tracking the amounts withdrawn. With Tšurikov, Defendant PLESHCHUK deleted and attempted to delete information on the RBS WorldPay computer network.

(b) Tšurikov was a computer hacker who during the relevant time period resided in or around Tallinn, Estonia. Tšurikov was responsible for reconnaissance of the RBS WorldPay computer network and for support of other hacking activity. Tšurikov was contacted by Defendant COVELIN regarding vulnerabilities in the RBS WorldPay computer network. Tšurikov shared this information with Defendant

PLESHCHUK. Tšurikov acted as liaison, connecting the hackers who found vulnerabilities on the computer network with Defendant PLESHCHUK, who could better exploit them. With Defendant PLESHCHUK, Tšurikov deleted and attempted to delete information on the RBS WorldPay computer network. Tšurikov also managed his own cashing group and provided fraudulently obtained card numbers and PIN codes to his group within Estonia. Cashers were individuals who used the fraudulently obtained payroll cards and PIN codes to obtain cash from ATMs. Tšurikov helped coordinate the receipt and distribution of proceeds.

(c) Defendant EVGENIY ANIKIN was a computer hacker who, in addition to his computer hacking activities in support of Defendant PLESHCHUK and Tšurikov, was responsible for managing the networks of cashers who used the fraudulently obtained payroll cards and PIN codes to obtain cash from ATMs on a coordinated time schedule. Defendant EVGENIY ANIKIN distributed fraudulently obtained prepaid payroll cards and their respective PIN codes to casher networks around the world. Defendant EVGENIY ANIKIN then managed the dividing of the proceeds and the distribution of cash from the cashers to other members of the scheme, including to Defendant PLESHCHUK, Tšurikov, and others.

(d) Defendant COVELIN was a computer hacker who during the relevant time period resided in or around Chişinău, Moldova. Defendant COVELIN learned of the vulnerability in the RBS WorldPay

computer network and provided the vulnerability (or "bug") to Tšurikov so that it could be exploited for financial gain. Defendants PLESHCHUK and ANIKIN, and Tšurikov, provided Defendant COVELIN a prepaid payroll card account number and associated PIN code, and raised the available funds on that account so Defendant COVELIN could make substantial withdrawals. Defendant COVELIN then distributed the account number and PIN code he was provided to others to fraudulently withdraw funds.

(e) Horohorin was a lead cashier who fraudulently withdrew RBSW funds from ATM(s) in or around Moscow, Russia. Horohorin at one point maintained Israeli and Ukranian passports.

(f) Sonya Martin was a cashier who obtained fraudulently obtained RBSW card account information from Chukukere. Using the fraudulently obtained card account information, Martin fraudulently withdrew RBSW funds from ATMs and provided cards with fraudulently obtained RBSW account numbers to others in or around Chicago, Illinois.

(g) Chukukere was a lead cashier who provided a fraudulently obtained RBSW card account number and PIN code to others, including Martin, intending that the information be used to make fraudulent withdrawals.

MEANS AND MANNERS

4. It was part of the conspiracy that:

(a) Beginning on or about November 4, 2008, Defendants PLESHCHUK, COVELIN, and ANIKIN, aided and abetted by each other and by others including, but not limited to, Tšurikov, gained unauthorized access from outside of the United States into the computer network of RBS WorldPay, located in the Northern District of Georgia. To gain unauthorized access, they used a vulnerability in the RBS WorldPay computer network that was provided to Tšurikov by Defendant COVELIN.

(b) During the period of on or about November 4, 2008, through on or about November 8, 2008, Defendants PLESHCHUK and ANIKIN, and Tšurikov, obtained, without authorization, information from the RBS WorldPay computer network, including prepaid payroll card numbers and PIN codes.

(c) Defendants PLESHCHUK and ANIKIN, and others, including, but not limited to, Tšurikov, distributed approximately 44 prepaid payroll card numbers and their respective PIN codes to networks of cashers. The lead cashers distributed the card numbers and PIN codes to individuals throughout the world, inside and outside of the United States. Of the 44 prepaid payroll card numbers distributed to the cashers, 42 of the numbers related to cards issued by Palm Desert National Bank.

(d) On or before November 8, 2008, Defendant PLESHCHUK, aided

and abetted by others, including, but not limited to, Defendant ANIKIN and Tšurikov, gained unauthorized access to the RBS WorldPay computer network and modified the data, raising the amount of funds available on the prepaid payroll card numbers they had fraudulently obtained and distributed. Also, Defendant PLESHCHUK, aided and abetted by others, including, but not limited to, Defendant ANIKIN Tšurikov, raised the limits that could be withdrawn from automated teller machines on the prepaid payroll card numbers they had distributed.

(e) On or about November 7, 2008, Defendants PLESHCHUK and ANIKIN, and Tšurikov, provided Defendant COVELIN with a payroll debit card account number and associated PIN code, and raised the available balance on that account number.

(f) On or about November 8, 2008, Defendant PLESHCHUK and Tšurikov provided Horohorin with a payroll debit card account number xxxxxxxxxxxx9488 and associated PIN code and raised the available balance on the account number to \$200,000.00. This RBSW payroll debit card account number was only assigned to Horohorin.

(g) On or about November 8, 2008, Defendant PLESHCHUK and Tšurikov provided Chukukere with a payroll debit card account number xxxxxxxxxxxx7662 and associated PIN code and at least twice raised the available balance on that account number. This RBSW payroll debit card account number was only assigned to Chukukere.

(h) On or about November 8, 2008, Defendants PLESHCHUK,

COVELIN, and ANIKIN, and Tšurikov notified the cashers, including Horohorin, Chukukere, and others, to whom they had distributed the fraudulently obtained payroll debit card numbers and PIN codes, to begin withdrawing funds.

(i) On or about November 8, 2008, Martin obtained payroll debit account number xxxxxxxxxxxx7662 and its associated PIN code from Chukukere. Using this information, Martin distributed cards containing the fraudulently obtained account number and PIN code to others and fraudulently withdrew funds from ATM terminals in or around Chicago, Illinois.

(j) With the limits raised, in the next approximately twelve hours at over 2,100 ATM terminals located in at least 280 cities around the world, including in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada, cashers used approximately 44 payroll debit cards to complete withdrawals worth over \$9 million in United States currency.

(k) Approximately \$125,739.30 was withdrawn from RBSW payroll debit card account number xxxxxxxxxxxx9488, assigned to Horohorin.

(l) Approximately \$1,010,317.68 was withdrawn from RBSW payroll debit card account number xxxxxxxxxxxx7662, assigned to Chukukere.

(m) While the cashers withdrew the funds, Defendant PLESHCHUK and Tšurikov accessed the RBS WorldPay computer network without authorization and monitored the withdrawals.

(n) After the withdrawals were completed, Defendant PLESHCHUK and Tšurikov sent computer commands from outside the United States to the RBS WorldPay computer network in the Northern District of Georgia, that destroyed data and attempted to destroy data on the RBS WorldPay computer network in an effort to, among other things, conceal their unauthorized access and fraud.

(o) The cashers were permitted to retain a percentage of the funds they had obtained, typically between 30% and 50%. The cashers returned the balance of the funds to the hackers, including Defendants PLESHCHUK and ANIKIN, and Tšurikov, using means such as WebMoney accounts and Western Union.

All in violation of 18 U.S.C. § 1349.

COUNTS TWO THROUGH TEN
(Wire Fraud)

5. The allegations contained in paragraphs 2 through 4 are re-alleged and incorporated as if fully set forth in this paragraph.

6. On or about the dates set forth below, in the Northern District of Georgia and elsewhere, Defendant VIKTOR PLESHCHUK, aided and abetted by Defendants OLEG COVELIN and EVGENIY ANIKIN, and by others whose identities are currently known and unknown to the Grand Jury, including, but not limited to, Sergei Tšurikov, for the purpose of executing and attempting to execute the aforesaid scheme and artifice, such scheme and artifice having been devised and intended to be devised to defraud, and to obtain money and property, by means of materially false and fraudulent pretenses, representations, and promises, did knowingly cause to be transmitted in interstate and foreign commerce, by means of a wire communication, certain signs, signals, and sounds, that is, the person listed in the table below, aided and abetted by the other Defendants and by others, did knowingly cause the following computer commands to be transmitted from outside of the United States to the computer network of RBS WorldPay in the Northern District of Georgia:

Count	Date	Person Sending Command	Computer Command (redacted)
-------	------	------------------------------	--------------------------------

2	Nov 7, 2008	PLESHCHUK	select top 100 * from xxxxLogS where xxxxLogID>2550000 AND xxxxPAN IN (xxxxxxx1627, xxxxxxxx6968, xxxxxxxx xxx5841, xxxxxxxx6050, xxxxxxxx0686, x xxxxxxx7540, xxxxxxxx7562, xxxxxxxx 4809, xxxxxxxx1905, xxxxxxxx6257, xxx xxxxxx7597, xxxxxxxx7217, xxxxxxxx739 9, xxxxxxxx5251, xxxxxxxx2851, xxxxxxx xxxxx9075, xxxxxxxx1597, xxxxxxxx8980, xxxxxxx3926, xxxxxxxx3964, xxxxxxxx xx5798, xxxxxxxx5100, xxxxxxxx1041, x xxxxxxx1782, xxxxxxxx3354, xxxxxxxx0 193, xxxxxxxx5010, xxxxxxxx2717, xxx xxxxxx8076, xxxxxxxx1992)
---	-------------	-----------	--

Count	Date	Person Sending Command	Computer Command (redacted)
-------	------	------------------------------	--------------------------------

3	Nov. 7, 2008	PLESHCHUK	<pre> select top 1000 * from xxxxxxxxxxxxtransaction where xxxxxxxxxxxxID>82300000 AND xxxxPAN IN ('xxxxxxxxxxxx1627', 'xxxxxxxxxxxx6968', 'xxxxxxx xxx5341', 'xxxxxxxxxxxx6050', 'xxxxxxxxxxxx0836', 'x xxxxxxxxxx7540', 'xxxxxxxxxxxx7662', 'xxxxxxxxxxxx 4809', 'xxxxxxxxxxxx51905', 'xxxxxxxxxxxx6257', 'xxxx xxxxxxxx7597', 'xxxxxxxxxxxx7217', 'xxxxxxxxxxxx6039 19', 'xxxxxxxxxxxx6251', 'xxxxxxxxxxxx2861', 'xxxxxxx xxxxx9075', 'xxxxxxxxxxxx1597', 'xxxxxxxxxxxx6980', 'xxxxxxxxxxxx3926', 'xxxxxxxxxxxx3964', 'xxxxxxxx xx5798', 'xxxxxxxxxxxx5100', 'xxxxxxxxxxxx1041', 'xx xxxxxxxxxx1782', 'xxxxxxxxxxxx3364', 'xxxxxxxxxxxx0 193', 'xxxxxxxxxxxx5010', 'xxxxxxxxxxxx2717', 'xxxxx xxxxxxxx8076', 'xxxxxxxxxxxx1992' </pre>
---	-----------------	-----------	--

4	Nov. 7, 2008	PLESHCHUK	<pre> UPDATE Card SET ATMxxxxxLimit=500000, POSxxxxxLimit=500000, ATMxxxx xxxxxx=500000, ATMxxxxxLimit2=500000, POSxxxxxLimit2=500000, ATMxx xxxxxxx2=500000 where xxxxPAN IN ('xxxxxxxxxxxx1627') </pre>
---	-----------------	-----------	---

Count	Date	Person Sending Command	Computer Command (redacted)
-------	------	------------------------------	--------------------------------

5	Nov 17 2008	PEESHCUK	delete from xxxxtlogs where xxxxtlogID>2400000 and xxxxPAN in (xxxxxxxxxxxx4809,xxxxxxxxxxxx3926,xxxxxxxx xxxx1041,xxxxxxxxxxxx5815,xxxxxxxxxxxx4912,xx xxxxxxxxxxxx9488,xxxxxxxxxxxx2840,xxxxxxxxxxxx 3890); delete from xxxxxxxxxxxxtransaction where xxxxxxxxxxxxID>32000000 and xxxxPAN in (xxxxxxxxxxxx4809,xxxxxxxxxxxx3926,xxxxxxxx xxxx1041,xxxxxxxxxxxx5815,xxxxxxxxxxxx4912,xx xxxxxxxxxxxx9488,xxxxxxxxxxxx2840,xxxxxxxxxxxx 3890); UPDATE Card SET ATMxxxxxlimit=505,POSxxxxxlimit=505,ATMxxxxxxx= 505, ATMxxxxxlimit2=5000,POSxxxxxlimit2=5000,ATMxxxxx xxx2=5000 where xxxxPAN in (xxxxxxxxxxxx4809,xxxxxxxxxxxx3926,xxxxxxxx xxxx1041,xxxxxxxxxxxx5815,xxxxxxxxxxxx4912,xx xxxxxxxxxxxx9488,xxxxxxxxxxxx2840,xxxxxxxxxxxx 3890);
---	-------------	----------	--

Count	Date	Person Sending Command	Computer Command (redacted)
6	Nov. 7, 2008	Tšurikov	select top 3 * from xxxxxxxxxxxTransaction where xxxxPAN= 'xxxxxxxxxxx5024' and xxxxxxxxxxDateTime > '11/01/2008'
7	Nov. 7, 2008	Tšurikov	select * from xxxxxxxxxxxTransaction where xxxxPAN='xxxxxxxxxxx5024' and xxxxxxxxxxDateTime > '11/01/2008'
8	Nov. 8, 2008	Tšurikov	select xxxxxxxxxxID,xxxxxxxxxxDateTime,xxxxxxxxxxAmount ,xxxxxxxxxxName,xxxxMerchxxxx,xxxxAddr,xxxxCity,xxx xState,xxxxZip,xxxxCounty from xxxxxxxxxxTransaction where xxxxPAN= 'xxxxxxxxxxx0336' and xxxxxxxxxxID>82300000
9	Nov. 8, 2008	Tšurikov	select xxxxxxxxxxID,xxxxxxxxxxDateTime,xxxxxxxxxxAmount ,xxxxxxxxxxName,xxxxMerchxxxx,xxxxAddr,xxxxCity,xxx xState,xxxxZip,xxxxCounty from xxxxxxxxxxTransaction where xxxxPAN='xxxxxxxxxxx0336' and xxxxxxxxxxID>82300000
10	Nov. 8, 2008	Tšurikov	delete from xxxxxLogs where xxxxxxxID>2400000 and xxxxPAN= 'xxxxxxxxxxx0336'

All in violation 18 U.S.C. §§ 1343 and 2.

COUNT ELEVEN

(Conspiracy to Commit Computer Fraud)

7. The allegations contained in paragraphs 2 through 4 are re-alleged and incorporated as if fully set forth in this paragraph.

8. From in or about November 4, 2008 through at least in or about November 25, 2008, in the Northern District of Georgia and elsewhere, Defendants VIKTOR PLESHCHUK, OLEG COVELIN, and EVGENIY ANIKIN, together with others known and unknown to the Grand Jury, including, but not limited to, Sergei Tšurikov, did knowingly and wilfully conspire to: (a) knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage and attempt to cause damage without authorization to a protected computer, causing loss aggregating at least \$5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, in violation of 18 U.S.C. §§ 1030 (a) (5) (A) and 1030(b); (b) intentionally access a computer without authorization, and thereby obtain information contained in a financial record of a financial institution, and of a card issuer as defined in 15 U.S.C. § 1602(n), and from a protected computer, and the offense being committed for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, specifically, conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349 and wire fraud in violation of 18 U.S.C. § 1343, and

the value of the information obtained exceeding \$5,000, in violation of 18 U.S.C. § 1030(a)(2); and (c) access a protected computer without authorization and by means of such conduct further the intended fraud and obtain value, specifically, prepaid payroll card numbers and PIN codes, and withdrawals from such prepaid payroll card accounts exceeding US\$9 million, in violation of 18 U.S.C. § 1030(a)(4);

All in violation of 18 U.S.C. § 371.

OVERT ACTS

9. In furtherance of the conspiracy and to achieve the objects thereof, the conspirators committed the following various overt acts among others, in the Northern District of Georgia and elsewhere:

(a) Defendant PLESHCHUK and Tšurikov took the actions described in Counts Two through Ten, issuing computer commands from outside of the United States to the RBS WorldPay computer network in the Northern District of Georgia.

(b) On or about November 4, 2008, Defendant COVELIN provided Tšurikov with knowledge of a vulnerability on the RBS WorldPay computer network located in the Northern District of Georgia.

(c) On or about November 4, 2008, Tšurikov accessed without authorization the RBS WorldPay computer network located in the Northern District of Georgia.

(d) On or about November 5, 2008, Defendants PLESHCHUK and COVELIN, and Tšurikov accessed without authorization the RBS WorldPay computer network located in the Northern District of Georgia.

(e) On or about November 5, 2008, Defendant COVELIN provided Defendant PLESHCHUK login information, including a password, to obtain access to a computer server on the RBS WorldPay computer network, located in the Northern District of Georgia.

(f) On or about November 7, 2008, Defendant PLESHCHUK obtained information from the RBS WorldPay computer network located in the Northern District of Georgia.

(g) On or about November 7, 2008, Defendant PLESHCHUK modified information on the RBS WorldPay computer network located in the Northern District of Georgia.

(h) On or about November 7, 2008, Defendant ANIKIN transferred account numbers and PIN codes obtained from the RBS WorldPay computer network to casher networks for their subsequent use at ATMs.

(i) On or about November 7, 2008, Defendant COVELIN received an account number and PIN code obtained from the RBS WorldPay computer network.

(j) On or about November 8, 2008, Defendant PLESHCHUK and Tšurikov accessed without authorization the RBS WorldPay computer network located in the Northern District of Georgia.

(k) On or about November 8, 2008, Defendant PLESHCHUK and Tšurikov deleted and attempted to delete information from the RBS WorldPay computer network located in the Northern District of Georgia.

COUNT TWELVE
(Computer Intrusion Causing Damage)

10. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendant VIKTOR PLESHCHUK, aided and abetted by Defendants OLEG COVELIN and EVGENIY ANIKIN, and by others known and unknown to the Grand Jury, including, but not limited to, Sergei Tšurikov, knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage and attempted to cause damage without authorization to a protected computer, causing loss aggregating at least \$5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(b), 1030(c)(4)(B), and 2.

COUNT THIRTEEN
(Computer Intrusion Obtaining Information)

11. On or about November 6, 2008, in the Northern District of Georgia and elsewhere, Defendant VIKTOR PLESHCHUK, aided and abetted by Defendants OLEG COVELIN and EVGENIY ANIKIN, and by

others known and unknown to the Grand Jury, including, but not limited to, Sergei Tšurikov, intentionally accessed a computer without authorization, and thereby obtained information contained in a financial record of a financial institution, and of a card issuer as defined in 15 U.S.C. § 1602(n), and from a protected computer, and the offense being committed for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, specifically, conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349 and wire fraud in violation of 18 U.S.C. § 1343, and the value of the information obtained exceeding \$5,000, in violation of 18 U.S.C. §§ 1030(a)(2), 1030(c)(2)(B)(i), 1030(c)(2)(B)(ii), 1030(c)(2)(B)(iii), and 2.

COUNT FOURTEEN
(Computer Intrusion Furthering Fraud)

12. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendants VIKTOR PLESHCHUK and EVGENIY ANIKIN, aided and abetted by Defendant OLEG COVELIN and by others known and unknown to the Grand Jury, including, but not limited to, Sergei Tšurikov, knowingly and with intent to defraud accessed a protected computer without authorization and by means of such conduct furthered the intended fraud and obtained value, specifically, prepaid payroll card numbers and PIN codes, and withdrawals from such prepaid payroll card accounts exceeding US\$9

million, in violation of 18 U.S.C. §§ 1030(a)(4), 1030(c)(3)(A), and 2.

COUNT FIFTEEN
(Aggravated Identity Theft)

13. On or about November 7, 2008, in the Northern District of Georgia and elsewhere, Defendants VIKTOR PLESHCHUK and EVGENIY ANIKIN, aided and abetted by each other, by Defendant OLEG COVELIN, and by others known and unknown to the Grand Jury, including, but not limited to, Sergei Tšurikov, during and in relation to the crime of wire fraud in violation of 18 U.S.C. § 1343, did knowingly transfer, possess, and use, without lawful authority, means of identification of other persons, that is, the Defendants, Tšurikov, and others knowingly transferred prepaid payroll card account numbers and associated PIN codes from the RBS WorldPay computer network located in the Northern District of Georgia, possessed the card account numbers and PIN codes, and transferred card account numbers and PIN codes to others for their use at ATM terminals, in violation of 18 U.S.C. §§ 1028A(a)(1), 1028A(b), 1028A(c)(5), and 2.

COUNT SIXTEEN
(Access Device Fraud)

14. The allegations contained in paragraphs 2 through 4, and paragraph 9, are re-alleged and incorporated as if fully set forth

in this paragraph.

15. On or about November 8, 2008, Sergei Tšurikov distributed fraudulently obtained prepaid payroll card numbers and PIN codes to Defendant IGOR GRUDIJEV, who, in turn, distributed the information to Defendants RONALD TSOI, EVELIN TSOI, and MIHHAIL JEVGENOV in Estonia. Together, Defendants RONALD TSOI, EVELIN TSOI, and MIHHAIL JEVGENOV withdrew funds worth approximately US\$289,000 from ATMs in Tallinn, Estonia. These transactions were debited on prepaid payroll card accounts on the RBS WorldPay computer system located in the Northern District of Georgia.

16. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendants RONALD TSOI, EVELIN TSOI, and MIHHAIL JEVGENOV, aided and abetted by Defendant IGOR GRUDIJEV and by others known and unknown to the Grand Jury, knowingly and with intent to defraud effected transactions with at least one access device issued to another person, that is prepaid payroll card account numbers and PIN codes which could be used, alone and in conjunction with another access device, to obtain money, goods, services, and other things of value, and that could be used to initiate a transfer of funds not originated solely by paper instrument, in order to receive payment and other things of value within a one-year period the aggregate of value of which was at least \$1,000, said offense affecting interstate and foreign commerce, in violation of 18 U.S.C. §§ 1029(a)(5),

1029(c)(1)(A)(ii), and 2.

COUNT THIRTY
(Conspiracy to Commit Bank Fraud)

17. From at least on or about November 4, 2008, through at least on or about November 25, 2008, in the Northern District of Georgia and elsewhere, the Defendants, VIKTOR PLESHCHUK, EVGENIY ANIKIN, VLADIMIR VALERYEVICH TAILAR, aka Vladamir Taliar, aka Vladamir Taylar, aka Vladamir Talyar, and ROMAN SELEZNEV, together with others known and unknown to the Grand Jury, including, but not limited to, Sergei Tšurikov, Vladislav Horohorin, Ezenwa Chukukere, and Sonya Martin, did knowingly conspire to devise a scheme and artifice:

- (1) to defraud a financial institution; and
- (2) to obtain any of the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of a financial institution, by means of false and fraudulent pretenses, representations, and promises;

all in violation of 18 U.S.C. § 1349.

BACKGROUND

18. The allegations contained in paragraph 2 are re-alleged and incorporated as if fully set forth in this paragraph.

CONSPIRATORS

19. The allegations contained in paragraph 3 are re-alleged and

incorporated as if fully set forth in this paragraph.

20. Defendants VLADIMIR VALERYEVICH TAILAR, aka Vladamir Taliar, aka Vladamir Taylar, aka Vladamir Talyar, and ROMAN SELEZNEV were lead cashers who were given fraudulently obtained RBSW card account numbers and PIN codes by others, including, but not limited to, Defendants VICTOR PLESHCHUK and EVGENIY ANIKIN and Sergei Tšurikov, and who then provided those fraudulently obtained RBSW card account numbers and PIN codes to others, intending that the information be used to make fraudulent withdrawals.

MEANS AND MANNERS

21. The allegations contained in paragraph 4 are re-alleged and incorporated as if fully set forth in this paragraph.

22. It was also part of the conspiracy that:

(a) On or about November 8, 2008, Defendants PLESHCHUK, ANIKIN, and others, including, but not limited to, Tšurikov, provided Defendant VLADIMIR VALERYEVICH TAILAR with RBSW payroll debit card account numbers xxxxxxxxxxxx3964, xxxxxxxxxxxx5798, and xxxxxxxxxxxx5100, and those accounts' associated PIN codes, and raised the available balances on those account numbers. These RBSW payroll debit card account numbers were only assigned to Defendant TAILAR.

(b) On or about November 8, 2008, Defendants PLESHCHUK, ANIKIN, and others, including, but not limited to, Tšurikov, provided Defendant ROMAN SELEZNEV with payroll debit card account

numbers xxxxxxxxxxxx5010, xxxxxxxxxxxx2717, xxxxxxxxxxxx3364, xxxxxxxxxxxx0193, and xxxxxxxxxxxx3786, and those accounts' associated PIN codes, and raised the available balances on those account numbers. These RBSW payroll debit card account numbers were only assigned to Defendant SELEZNEV.

(c) On or about November 8, 2008, Defendants PLESHCHUK, ANIKIN, and others, including, but not limited to, Tšurikov, notified the cashers, including Defendants TAILAR and SELEZNEV, and others, to whom they had distributed the fraudulently obtained payroll debit card numbers and PIN codes, to begin withdrawing funds.

(d) RBSW records show that a total of approximately \$872,213.30 was withdrawn from the RBSW payroll debit card account numbers assigned to Defendant TAILAR.

(e) RBSW records show that approximately \$2,178,349 was withdrawn from the RBSW payroll debit card account numbers assigned to Defendant SELEZNEV.

All in violation of 18 U.S.C. § 1349.

COUNT THIRTY-ONE
(Bank Fraud)

23. The allegations contained in paragraphs 2 through 4, and paragraphs 9, 20, and 22, are re-alleged and incorporated as if fully set forth in this paragraph.

24. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendant VLADIMIR TAILAR, aka Vladamir

Taliar, aka Vladamir Taylar, aka Vladamir Talyar, aided and abetted by others known and unknown to the Grand Jury, knowingly executed and attempted to execute, and knowingly aided and abetted, the execution and attempted execution of, a scheme and artifice (1) to defraud a financial institution, and (2) to obtain moneys, funds, and assets owned by and under the custody and control of a financial institution by means of materially false and fraudulent pretenses, representations and promises, that is, for the purpose of executing and attempting to execute the aforesaid scheme and artifice, Defendant TAILAR did knowingly cause fraudulent ATM withdrawals to be made from RBSW prepaid payroll account numbers xxxxxxxxxxxx3964, xxxxxxxxxxxx5798, and xxxxxxxxxxxx5100, representing accounts with Palm Desert National Bank, that were processed using the computer network of RBSW in the Northern District of Georgia.

All in violation 18 U.S.C. §§ 1344 and 2.

COUNTS THIRTY-TWO THROUGH THIRTY-EIGHT
(Wire Fraud)

25. The allegations contained in paragraphs 2 through 4, and paragraphs 9, 20, and 22, are re-alleged and incorporated as if fully set forth in this paragraph.

26. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendant VLADIMIR TAILAR, aka Vladamir Taliar, aka Vladamir Taylar, aka Vladamir Talyar, aided and abetted by others known and unknown to the Grand Jury, for the

purpose of executing and attempting to execute the aforesaid scheme and artifice, such scheme and artifice having been devised and intended to be devised to defraud, and to obtain money and property, by means of materially false and fraudulent pretenses, representations, and promises, did knowingly cause to be transmitted in interstate and foreign commerce, by means of a wire communication, certain signs, signals, and sounds, that is, the Defendant knowingly caused wires signaling the following requests for the withdrawal of funds from fraudulently obtained RBSW prepaid payroll card account numbers xxxxxxxxxxxx3964, xxxxxxxxxxxx5798, and xxxxxxxxxxxx5100, to be transmitted from outside of the United States to the computer network of RBSW in the Northern District of Georgia, such scheme and artifice affecting a financial institution:

Count	Last four digits of card number	Location of ATM withdrawal	Local Time at Location of ATM Withdrawal (at or about)	Amount (U.S.D.)
32	3964	Lugansk, Ukraine	09:21:02	\$692.04
33	3964	Lugansk, Ukraine	09:21:47	\$692.04
34	3964	Lugansk, Ukraine	09:22:29	\$692.04
35	3964	Lugansk, Ukraine	09:23:11	\$692.04
36	3964	Lugansk, Ukraine	09:23:56	\$692.04
37	5100	Southampton, U.K.	12:01:09	\$786.77
38	5798	Zhukomyi, Ukraine	12:04:03	\$692.04

All in violation 18 U.S.C. §§ 1343 and 2.

COUNT THIRTY-NINE
(Bank Fraud)

27. The allegations contained in paragraphs 2 through 4, and paragraphs 9, 20, and 22, are re-alleged and incorporated as if fully set forth in this paragraph.

28. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendant ROMAN SELEZNEV, aided and abetted by others known and unknown to the Grand Jury, knowingly executed and attempted to execute, and knowingly aided and abetted, the execution and attempted execution of, a scheme and artifice (1) to defraud a financial institution, and (2) to obtain moneys, funds, and assets owned by and under the custody and control of a financial institution by means of materially false and fraudulent pretenses, representations and promises, that is, for the purpose of executing and attempting to execute the aforesaid scheme and artifice, Defendant SELEZNEV did knowingly cause fraudulent ATM withdrawals to be made from RBSW prepaid payroll account numbers xxxxxxxxxxxx5010, xxxxxxxxxxxx2717, xxxxxxxxxxxx3364, xxxxxxxxxxxx0193, and xxxxxxxxxxxx3786, representing accounts with Palm Desert National Bank, that were processed using the computer network of RBSW in the Northern District of Georgia.

All in violation 18 U.S.C. §§ 1344 and 2.

COUNTS FORTY THROUGH FORTY-FOUR
(Wire Fraud)

29. The allegations contained in paragraphs 2 through 4, and paragraphs 9, 20, and 22, are re-alleged and incorporated as if fully set forth in this paragraph.

30. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendant ROMAN SELEZNEV, aided and abetted by others known and unknown to the Grand Jury, for the purpose of executing and attempting to execute the aforesaid scheme and artifice, such scheme and artifice having been devised and intended to be devised to defraud, and to obtain money and property, by means of materially false and fraudulent pretenses, representations, and promises, did knowingly cause to be transmitted in interstate and foreign commerce, by means of a wire communication, certain signs, signals, and sounds, that is, the Defendant knowingly caused wires signaling the following requests for the withdrawal of funds from fraudulently obtained RBSW prepaid payroll card account numbers xxxxxxxxxxxx5010, xxxxxxxxxxxx2717, xxxxxxxxxxxx3364, xxxxxxxxxxxx0193, and xxxxxxxxxxxx3786, to be transmitted from outside of the United States to the computer network of RBSW in the Northern District of Georgia, such scheme and artifice affecting a financial institution:

Count	Last four digits of card number	Location of ATM withdrawal	Local Time at Location of ATM Withdrawal (at or about)	Amount (U.S.D.)
40	2717	Bangkok, Thailand	15:44:53	\$287.02
41	0193	Auckland, New Zealand	22:45:38	\$472.07
42	3786	Moscow, Russia	12:00:32	\$277.53
43	5010	Hong Kong	16:16:07	\$774.22
44	9364	Leeds, U.K.	11:50:16	\$692.35

All in violation 18 U.S.C. §§ 1343 and 2.

FORFEITURE

31. As a result of committing an offense as alleged in Counts 1-14, 16, and 30-44 of this Indictment, the Defendants shall forfeit to the United States pursuant to Title 18, United States Code, Section 982(a)(2) any property, real or personal, which constitutes or is derived from proceeds obtained directly or indirectly, as the result of said offenses as alleged in this Indictment, including, but not limited to a sum of money representing the amount of proceeds obtained as a result of the offense, of at least \$9,477,146.67 in United States currency.

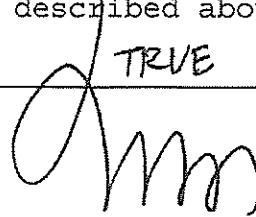
In addition, as a result of an offense as alleged in Counts 16 of this Indictment, the Defendants shall forfeit to the United States pursuant to Title 18, United States Code, Section 1029(c) any personal property used or intended to be used to commit the offense(s).

If any of the above-described forfeitable property, as a result of any act or omission of the defendant(s):

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty;

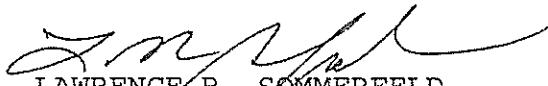
it is the intent of the United States, pursuant to 21 U.S.C.
§ 853(p) as incorporated by 18 U.S.C. § 982(b), to seek
forfeiture of any other property of said defendant(s) up to the
value of the forfeitable property described above.

A TRUE BILL

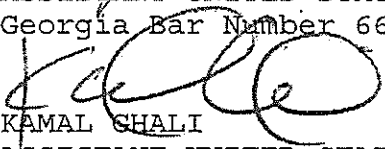


FOREPERSON

SALLY QUILLIAN YATES
UNITED STATES ATTORNEY



LAWRENCE R. SOMMERFELD
ASSISTANT UNITED STATES ATTORNEY
Georgia Bar Number 666936



KAMAL CHALI
ASSISTANT UNITED STATES ATTORNEY
Georgia Bar Number 805055

600 U.S. Courthouse
75 Spring Street, S.W.
Atlanta, GA 30303
Telephone 404-581-6000